doi:10.3969/j.issn.1000-436x.2012.12.004

基于 UDP 流量的 P2P 流媒体流量识别算法研究

董仕[1,2,3,4]，王岗[2,3,4]

(1. 周口师范学院 计算机科学与技术学院，河南 周口 466001；2. 东南大学 计算机科学与工程学院，江苏 南京 210092；
3. 江苏省计算机网络技术重点实验室，江苏 南京 210092；4. 国家教育部计算机网络和信息集成重点实验室，江苏 南京 210092)

摘 要：以几款主流的 P2P 流媒体网络电视作为研究对象，深入分析了其产生的流量在端口使用方面的特点和报文长度分布上的差异。通过对这些特征的总结和提取，获得了基于端口特性“在一次交互过程中，特定主机的特定端口唯一确定一种应用”等结论。在此基础上提出了一种基于带有扩展属性的流记录准确识别 P2P 应用 UDP 流量的 EXID 算法。通过对 CERNET 江苏省边界 10G 主干信道上采集的 Trace 数据中 5 种 P2P 流媒体应用进行识别，并与机器学习流量识别算法进行比较，其结果表明提出的方案具有很高的查准率和查全率，时间效率高，且不易受样本比重的影响。

关键词：UDP；P2P；流量识别；扩展的流记录

中图分类号：TP393.08 **文献标识码：**A **文章编号：**1000-436X(2012)12-0025-10

Research on P2P streaming media identification based on UDP

DONG Shi[1,2,3,4], WANG Gang[2,3,4]

(1. School of Computer Science and Technology, Zhoukou Nor l University, Zhoukou 466001, China;
2. College of Computer Science and Engineering, Southeast University, Nanjing 210092, China;
3. Jiangsu Provincial Key Laboratory of Computer Network, Nanjing 210092, China;
4. Key Laboratory of Computer Network and Information Integration, Ministry of Education, Nanjing 210092, China)

Abstract: Several popular P2P networks TV were studied, and their differences in port usage and packet size distribution were analyzed thoroughly. By observing the above characteristics, the conclusions that network TV application employs only one port to generate most of UDP traffic in one communicat period were summarized, and the UDP packet sizes in various network TV differ significantly. Thus, a method that can identify P2P application's UDP traffic accurately and effectively was proposed based on extended flow records. Through identifying and verifying the five P2P streaming application traffic which was called Trace data collected from the backbone channel of CERNET (China education and research network) border in Jiangsu Province, and traffic identification results compared with machine learning algorithms show that the proposed method has a high precision rate and recall rate, high time efficient, and not susceptible to the impact of the proportion of the sample.

Key words: UDP; P2P; traffic identification; extended flow records

收稿日期：2011-10-17；**修回日期：**2012-04-16

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目(2009CB320505); **国家科技支撑计划基金资助项目**(2008BAH37B04)

Foundation Items: The National Basic Research Program of China (973 Program) (2009CB320505); The National Science and Technology Plan Program of China (2008BAH37B04)

1 引言

网络技术的成熟和互联网带宽的不断增长使得P2P应用越来越普及，如何有效地管理和控制网络中的P2P流量，以保证其他网络业务的需要并使网络得以正常运行已成为目前网络管理中必须要面对的一个问题。据统计中国国内互联网流量中UDP比例已接近50%[1,2]，而西方国家同期的数据大约仅为20%[3,4]。国内互联网UDP流量比例远高于西方的主要原因是由于国内P2P应用被广泛使用。高UDP比例流量网络的运行风险要更高，这是因为当拥塞发生时，UDP流量会对TCP流量产生抑制[5]，而网络上所有重要数据均采用TCP传递。所以对P2P流量进行有效的管理在中国显得更加重要。

对P2P流量进行有效管理的前提是对P2P流量的准确识别。目前传统的应用类型识别主要分3类：基于端口[6]、基于机器学习[7~11]和基于深度报文检测(DPI)[12~15]。P2P应用普遍使用随机动态端口，基于特定端口的检测方法已不适用，而DPI方法基于全报文检测需要已知特征码，对加密P2P应用束手无策。基于机器学习的方法可以在流层面完成基于流量行为特征检测，但算法复杂度高，识别率低，漏报率和误报率较大。目前并没有一个能够得到公认的有效面向P2P应用的识别算法。本文的研究工作围绕P2P流量识别这个基本问题展开，研究工作基于扩展的流记录进行。与上述所有的研究方法不同的是，本文的核心思路是用时间粒度聚合并揭示P2P应用在实际使用过程中因为“流控”和“并发”所体现出的特性，并据此将其标识。选择具有代表性的以UDP作传输层协议的几款P2P网络电视为研究对象，希望能将其准确地从流量中标识出来。在详细讨论了算法后，文中采用在“峰时”和“谷时”长度分别为1h的实测IP TRACE作为实验，结果表明采用EXID算法识别结果查准率和查全率均超出97%。并与比较流行的机器学习识别算法进行了比较，结果表明采用此识别算法在查准率上优于机器学习识别算法，有很高的总体正确率，且不易受到样本比重的影响。

2 相关工作

目前的P2P流量识别方法主要包含4种：端口识别、深层数据分组检测、基于机器学习的流量识别、基于传输层连接模式的识别。

2.1 端口识别

早期的P2P应用程序使用固定的端口号，所以网络服务提供商(ISP)常利用固定端口号识别P2P流量。然而目前的P2P应用程序使用端口跳变技术和端口伪装技术来躲避流量检测。Bleul等[16]分析DirectConnect网络得出，在已观察到的端口中，70%的端口仅仅被使用了一次。可见，基于端口的P2P流量识别技术已不能满足当前需求。

2.2 深层数据分组检测(DPI)

DPI技术常采用模式匹配算法搜索流量载荷中P2P协议的特征值，进而通过特征匹配判断是否属于该P2P流量。流量载荷特征提取是确保DPI识别准确率的关键，而模式匹配算法是确保DPI执行效率的关键。

目前,基于DPI技术的P2P流量识别研究主要通过改进模式匹配算法来提高DPI技术的吞吐量。Sen等设计了一个基于模式匹配算法的在线分类器识别P2P流量，并评估了SR(standard regex)算法、AR(AST regex)算法和KR(Karp-Rabin)算法的流量识别性能，其吞吐量分别为0.21%~2.39%、8.7%~77.60%和0.07%~0.9%。可见，AR算法的性能相对最好。Xu等[17]利用Rabin字符串匹配算法搜索主机上传流量和下载流量中是否存在相同的负载内容，如果存在相同的负载内容，则认为该主机为P2P主机。实际上，为了保证DPI健壮性，模式匹配算法常常要结合其他技术，例如流状态跟踪、协议状态检测机制等。

综上所述，在大多数情况下，DPI技术准确性高、可靠性好，且能够细粒度地识别流量，主要适合于非加密流量的识别，其识别的准确性依赖于特征库的更新。而学术界也常以该技术作为新流量识别方法的比较基准。L7-filter能够准确识别128种协议流量，但对负载加密的Skype流量和迅雷流量识别能力有限。文献[18]中识别负载加密的emule流量，其准确性仅在30%~70%之间。此外，在实际应用中，由于DPI技术侵犯个人隐私，其应用面受到限制。

2.3 基于机器学习的流量识别

基于机器学习的流量识别一般不依赖于应用层负载信息，它利用流量统计特征作为属性，建立机器学习分类模型识别P2P流量。P2P流量的统计特征提取可以从数据分组级和数据流级提取。

1) 数据分组特征

数据分组特征主要统计单个流内数据分组大小、数据分组到达的间隔时间、数据分组比率(单位时间内传输数据分组的个数)等。Bleul 等比较分析 Bittorrent、DirectConnect、eDonkey、Gnutella 以及 FastTrack 这 5 种 P2P 流量发现，它们之间的平均数据分组长差异较大。除了 eDonkey 协议外，其他 4 种频繁出现长度是小于 200byte 的数据分组。Teufl 等[19]指出，音频流的分组到达间隔时间非常相似。Marcell 等[20]对 Skype 呼叫流量进行实验分析，发现平均语音数据分组大小在 40~320byte 之间变化，单向讲话流的带宽在 20~80kbit/s 之间变化，而 Skype 语音数据分组到达的时间间隔是 30ms 或者 60ms，相应的数据分组比率分别是 33 个数据分组/s 和 16 个数据分组/s。它们利用这些特征将 Skype 流量与其他的 VoIP 流量(MSN、YahooMessenger、AOL Messenger、Gtalk)区分开。Bonfiglio 等[21]对 Skype 流量进行实验分析发现，在 Skype 呼叫连接的前 30s 内，Skype 客户端发送的数据分组大小大约是以后发送数据分组大小的 2 倍，平均数据分组到达时间间隔是 20ms、30ms 或者 60ms。它们对 Skype 流量识别的误报率为 0~0.01%，漏报率为 9.82%~29.98%。Yang 等[22]统计分组长度、分组到达时间间隔和分组的字节数等特征，对 Bittorrent 流量、pplive 流量、Skype 流量和 MSN 流量的识别准确性在 91%~95%。Este 等[23]研究了数据分组特征的时空稳定性，发现数据分组大小受到网络时空环境变化的影响相对最小，而且每个 TCP 连接成功后的第 1 个数据分组大小对分类的贡献最大。它们仅分析了 TCP 协议下的数据分组特征稳定性，对于 UDP 协议下的特征稳定性未进行深入研究。文献[24]利用数据分组大小和数据分组方向(客户端发送的数据分组为正，服务器发送的数据分组为负)分类网络流，对 Bittorrent 的识别准确率为 96.8%。此外，Roughan 等[25]的研究表明：仅统计数据分组特征还不足以区分大数据块流和流媒体，也不能将 FTP 流与 WWW 流区分开，因此还需要在数据流级获取更多的统计特征。

2) 数据流特征

数据流特征主要包括流的源/目的端口号、流大小、流持续时间以及标识位(FIN、SYN、RST、PUSH、ACK、URG)被设置的 TCP 数据分组数目等。流大小是指同属于一个数据流的所有数据分组字节数总和。流持续时间由一个流的结束时刻减去流开始时刻得到。一般而言，TCP 流的开始时刻是其 SYN 数据分组到达时刻，TCP 流的结束时刻是其 FIN 或 RST 数据分组到达时刻。UDP 流的开始时刻和结束时刻还没有明确定义，目前，Cisco Netflow 将流的超时值设置为 60s。即，连续 2 个 UDP 数据分组到达时间间隔超过 60s 则认为是 2 个流。目前，对于数据流特征提取，国内外学术界已有大量工作。文献[26,27]对 P2P 数据流和 Web 数据流的统计特征进行了比较分析，发现 P2P 流大小的均值比 Web 流大小的均值大，P2P 流的平均持续时间要比 Web 流的平均持续时间长。陈庆章等[28]指出 FTP 流量和 P2P 流量各自的数据流特征，发现 P2P 流的数据分组大小变化幅度更大，流的持续时间更长，流的总长度更大。Moore 等[29]提取 249 种 TCP 数据流特征，将网络流量粗略分成 10 种类别，采用 BAYES+NBK 识别 Web 流量的准确性高达 99.27%，而对 P2P 文件共享流量(KazaA，Bittorrent，Gnutella)识别准确性仅达到 36.45%。由于 249 维特征向量有较大的计算开销和存储开销，Li[30]利用基于相关的快速特征选择算法(FCBF, fast correlation-based filter)从 249 种数据流特征中选出 12 种 TCP 流特征。此外，Li 还提取了 9 种 UDP 流特征。Erman 等[31]用向后贪婪特征选择算法从 25 种 TCP 数据流特征中选择 11 种流特征。

2.4 基于 P2P 传输层连接模式识别

针对不同的网络行为特征可以设计出多种流量识别算法，本节介绍一些基于传输层连接模式的识别算法。Sen 等[32]查阅大量的 P2P 协议相关文档，提取出 Gnutella，KazaA，DirectConnect，BitTorrent，eDonkey 等 5 种 P2P 文件共享流量特征，识别准确率在 90.1%~100%。手工方式提取特征比较耗时，对于协议文档不公开或加密的流量，获取特征更加困难。Karagiannis 等[33]发现，P2P 网络传输层连接的 2 个特征：一是大约 2/3 的 P2P 应用同时使用 TCP 和 UDP 协议，而其他少数应用中同时使用 2 种协议的仅仅包括 NetBIOS、DNS、游戏等，这些少数应用大多使用固定的端口进行通信，例如 NetBIOS 使用 135、137、139 和 445 端口，通过端口号可排除掉这些非 P2P 应用；二是在 P2P 文件共享网络中。对等体之间通常仅使用一条 TCP 连接进行文件传输；而对于 Web 等非 P2P 应用，客户端和服务器之间通常存在多条并发的 TCP 连接。Karagiannis 利用

这 2 个特征识别 P2P 流量，其误报率在 80%~12%之间[34]。针对对等网络(P2P)中技术网络的分布式特点，依据节点在单位时间内连接的目的子网数量(*d* 值)和节点单位时间内连接的目的 IP 数目与有效连接数目的比值(*m* 值)特性，提出一种基于节点连接特性的 P2P 节点识别算法。P2P 节点的 *d* 值和 *m* 值都明显大于其他节点(如典型的 HTTP 节点)，并存在一个阈值区间，据此可高效识别 P2P 节点。在清华大学校园网上的实验结果显示，该算法比当前主流的算法识别效果更好，节点误识别率和丢失率都小于 5%。目前虽然对 P2P 应用识别已经取得了很多研究成果，但是针对 P2P 流媒体识别的研究却很少，因此本文针对目前流行的 5 种 P2P 流媒体进行特征发现并提出了一种流量识别算法。

3 行为特征分析

针对当前流行的 5 种 P2P 流媒体：PPS 点播、PPLIVE、UUSEE、QQLIVE 和皮皮点播分别进行研究，并对 P2P 流媒体进行了大量的抓分组分析，总结和归纳了 2 个特征，分别介绍如下。

3.1 同一端口特征

本特征为共性特征。所有这些 P2P 软件在使用过程中虽然以随机方式选择端口，但在一次使用（点播或直播）过程中，无论与多少个对象进行交换，均使用同一个本地非系统端口。这个特性可以进一步描述为：一个 IP 地址为 *X* 的主机发起的一次 P2P 交互，无论与多少个对端主机进行交互，均使用一个相同的本地端口 *Y*（*Y*>1 023）。

命题 1 一个地址为 *X* 的主机发起的一次 P2P 交互所产生所有流记录的五元组均具有（*X*,*Y*,*,*,UDP）或（*,*,*X*,*Y*,UDP）的特征，其中，*Y* 为一个大于 1 023 的固定值，*代表一个任意的 IP 地址或端口。

基于这个特征和所有应用只能选择未被正在使用的端口这个基本原理，可以将一个时间段内所有符合条件的流记录按 P2P 交互划分集合，每个集合中的所有流记录属于同一个 P2P 活动，当然也属于同一个 P2P 应用。这个命题的意义在于对 P2P 的识别可以在这个流记录集合的层面上进行，只要可以准确识别集合中的一个流记录就可以使所有的流记录得到标识，另一方面也可以利用整个集合体现出的特性进行标识。

3.2 报文长度和流控特征

P2P 应用在获得 UDP 协议带来好处的同时，也失去 TCP 协议的一些优点，其中之一就是流控，TCP 协议使用滑动窗口机制完成这项工作，单纯的 UDP 没有类似的功能。流控显然是 P2P 应用必须具备的一项功能，这是因为通过端系统的观察，发现所有 P2P 软件的所有下载过程均呈现双向的 UDP 连接，但在流量（报文长度）上呈现出明显的差异。由于没有滑动窗口机制的支持，每个 P2P 应用各自选择了一组固定的报文长度，不同的应用其选择各自不同。图 1 描述了 5 种不同应用的报文长度按频率所占的比重降序排列，取比重较大的前 4 个报文长度进行观察和分析，从识别算法实现方便的角度，笔者根据观察实测数据，选择了各种 P2P 应用最长报文和最短报文作为识别特征。每个应用具体确定的数字如表 1 所示。

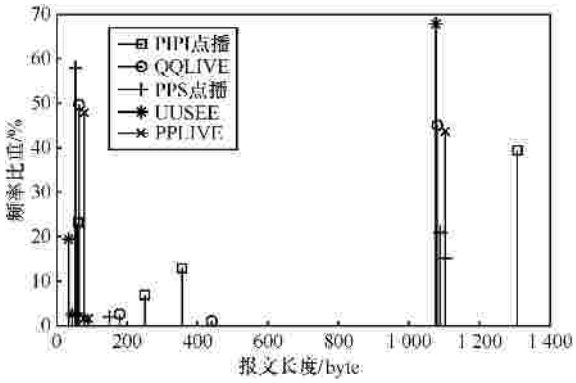

图 1 5 种 P2P 应用的频率比重分布

表 1 P2P 应用的最大最小报文长度

应用类型	报文数量	大报文长度集合	小报文长度集合
PPS 点播	401 448	{1 104,1 151,1 136}	{53,45}
PPLIVE	109 742	{1 103，1 257}	{73, 77, 58}
UUSEE	37 102	{1 076}	{36}
QQLIVE	145 363	{1 080,1 122}	{ 41, 57, 63}
皮皮点播	44 431	{1 308}	{38, 40}

4 EXID 流量识别算法

本文的识别算法依据第 3 节总结和归纳的特征，并基于扩展的流记录格式对网络流量进行识别。

4.1 扩展流记录定义

流记录是对面向会话报文集合的描述。最早从学术研究角度提出的流记录判定标准为五元组超

时，基本的流记录数据还包括起始时间、终止时间、流内字节数和流内报文数四项。思科公司基于路由器实现的 NetFlow[14]中，在此基础上扩展了 TOS、下一跳路由器地址、源宿 AS 等字段。

本文识别算法使用另外一种扩展的流记录，扩展项为流内最长报文字节数和最短报文字节数，具体描述如下。

定义 1　扩展流记录 FLOWS1 的格式为八元组（*sip*，*dip*，*sport*，*dport*，*prot*，*lastime*，*lgest*，*shest*），其中，*lastime* 为流终止时间，*lgest* 为流内最长报文长度，*shest* 为流内最短报文长度。

4.2　EXID 识别算法

算法的输入是格式为 FLOWS1 的流记录集合 *Flow*，核心思路是将输入的流记录根据 *lastime* 和给的时间粒度参数 *t*，划分成不同的子集，在此基础上对子集内的流记录根据 3.1 节的特征进行聚类，然后根据 3.2 节的个性特征确定每个类所属的应用。

定义 2　设有一个任意给定的 *t* 和一个 FLOWS1 格式的流记录集合 *Flow*，令 *Maxlastime* 和 *Minlastime* 为 Flow 中所有流记录的最大、最小 *lastime* 值，$n=(MaxLastime- MinLastime)/t$，则可根据流记录的 *lastime* 将 *Flow* 划分成 *n* 个子集合$\{flow_1,flow_2,\cdots,flow_i,\cdots,flow_n\}$，其中，任意一个，$flow_i$ 称为该 *Flow* 的第 *i* 个时间粒度子集。

根据这个定义，可得出结论：如果 *Flow* 中的流记录 R_x 和 R_y 属于同一个时间粒度子集，$flow_i$，则 $|R_x.lastime - R_y.lastime| \le t$。还可以得到如下。

命题 2　流记录集 *Flow* 的时间粒度子集，$flow_i$ 构成 Flow 的完整划分。

定义 3　*Flow* 的时间粒度子集，$flow_i$ 中的任意流记录 R_x 和 R_y，如果满足

$$R_x(sip,sport)=R_y(sip,sport)$$

或 $R_x(sip,sport)=R_y(dip,dport)$

或 $R_x(dip,dport)=R_y(dip,dport)$

则 R_x 和 R_y 属于 $flow_i$ 的同一个聚类，表示为 $flow_{i\_}set_j(IP,port)$

根据 3.1 节中的命题 1，$flow_{i\_}set_j(ip,port)$ 中的所有流记录属于同一次 P2P 交互，它们属于同一种 P2P 应用。

由于主机端口不能并发使用，一台主机的一个端口在同一时刻只能与唯一的另一台主机通信，实际上本文算法是利用了这个特征来聚类流记录并识别其应用的。设一个客户端口在一次使用完毕后，在时间粒度 *t* 内再次被使用的概率为 *p*，则一个流记录 R_X 同时属于 2 个聚合集的概率小于 *p*。假设一台参与交互的 P2P 主机平均每 ? *t* 需要使用一个新端口，平均正在使用的端口数量为 *N*，本地流的平均持续时间为则 $p<t/(? t/(65\ 536- 1\ 024- N))$。如果取 ? *t*=5，*t*=5min，*N*=512，则 *p*<0.1%。

设持续时间小于 *t* 时间内的同类流比例为 *q*。根据观察，持续时间小于 5min 的点播流的比例小于 30%，这样 2 个条件同时成立的可能性为 *pq*<0.02%，即认为一个 $flow_i$ 中流记录 R_x 只可能属于一个聚类。下面给出具体的聚类及识别算法，分成聚类中双向流报文长度对（pairs）生成算法和核心标识 EXID 识别算法由 2 部分组成，分别是报文长度对（pairs）生成算法 BFPS 和核心识别算法。

算法 1　报文长度对生成算法

//输入：一个聚类 $flow_{i\_}set_j$

//输出：报文长度对集 *BFPS*（$flow_{i\_}set_j$），该集合的元素是二元组（*Lgest*,*Shest*）

BFPS ($flow_{i\_}set_j$)

{

输入聚类集合 $flow_{i\_}set_j$ 为 *s*，初始化报文对集合 *BFPS*

do {

S:= $flow_{i\_}set_j$; *BFPS*:={};

While *S*<>{}

从 *S* 中选择一个记录 *R*;　*S*:=*S*- {*R*};

Lgest:=*R.lgest*; *Shest*:=*R.shest*

For *S* 中所有的记录 *Rx*

If　(*R* 的五元组=*Rx* 的五元组) 或

(*R.sip*,*R.sport*)=(*Rx.dip*,*Rx.dport*)或

(*R.dip*,*R.dport*)=(*Rx.sip*,*Rx.sport*)

Then[*Lgest*:=max(*Lgest*, *Rx.lgest*);

Shest:=min(*Shest*, *Rx.shest*)；

S:=*S*- {*Rx*}]

BFPS: =*BFPS*+{(*Lgest*, *Shest*)}

End while

}

上述算法的目的是对相同 5 元组的流进行快速有效地合并，并根据 3.2 节中提出的流控特征，寻找并合并聚类中的双向流，给出所有双向流的最长、最短报文对，以便下面的核心算法利用 3.2 节

中的报文长度特征进行识别。

算法2 报文长度特征识别算法

//输入：一个FLOWS1格式的流记录集合*Flow*，时间粒度*t*

//输出：带应用标记的*Flow*

Identification_app ($flow_i\_set_j$)

{

输入聚类集合 $flow_i\_set_j$ 为 *s*，初始化报文对集合 *BFPS*

do {

for every $< flow\_port, flow\_pro >$ in $flow_i\_set_j$

// Step 1. 从*Flow*中选择源宿端口均大于1 023的且*prot*为UDP的记录，将其余记录标识为0(未识别)

If (*flow_port*>1 023 且 *flow_pro*=*udp*)

S:= $flow_i\_set_j$; *BFPS*:={};

While *S*<>{}

从*S*中选择一个记录*R*; *S*:=*S*- {*R*};

求出 *n*=(*MaxLastime*- *MinLastime*)/*t*

生成*n*个流记录 $flow_1,\cdots,flow_n$

// Step2: 将其余的流记录根据定义2和*t*分割成时间粒度子集 $flow_i$

Lgest:=*R.lgest*; *Shest*:=*R.shest*

If Rx（*sip*，*sport*）= *Ry*（*sip*，*sport*）或

Rx（*sip*，*sport*）= *Ry*（*dip*，*dport*）或

Rx（*dip*，*dport*）= *Ry*（*dip*，*dport*）

Then

$flow_i\_set_j \leftarrow < flow(ip, port) >$

// Step3 根据定义3构造每个 $flow_i$ 的所有聚类 $flow_i\_set_j$

for every $flow_i\_set_j$

$< Max_{ij}, Min_{ij} > \leftarrow BFPS(flow_i\_set_j)$

// Step4：对每个 $Flow_i\_Set_j$，根据聚合中双向流报文长度对（pairs）生成算法，获得它的 $BFPS_{ij}$，设 $BFPS_{ij}$ 中的任意元素为（Max_{ij}, Min_{ij}），则聚合集 $Flow_i\_Set_j$ 的标记值 $Flag_{ij}$：

$$Flag_i = \begin{cases} V_n \ (\exists Max_{ij} \in PMax_n \ \&\& Min_{ij} \in PMin_n) \text{ 上} \\ (\text{P2P 应用 } n) \\ 0 \ (\forall Max_{ij} \notin PMax_n \ || \ Min_{ij} \notin PMin_n) \text{ 上} \\ (\text{未知应用}) \end{cases}$$

// Step5:将 $Flag_{ij}$ 标记到该聚合中的每个流记录

通过选择合适的散列函数，可以将上述的时间复杂性控制在 *o*(|*Flow*|)

End while

}

4.3 算法时空复杂度分析

EXID识别算法主要分2步：聚类和识别。聚类过程时间复杂度为流*S*数*n*的线性函数，即为*O*(*n*)。而识别过程时间复杂度也为*O*(*n*)，因此，总的算法复杂度为*O*(*n*)+*O*(*n*)，由于聚类的时候，需要*k*个最大报文长度*Lgest*的数目和*k*个最小报文长度*Shest*的数目，因此需要的空间复杂度为*O*(*k*)，在识别过程中因为需要存储5对最大和最小的报文长度，这将占据空间复杂度为*O*(2×5)，另外总的聚类和识别程序本身所占的空间复杂度为*O*(*n*)，因此总的空间复杂度为*O*(*k*)+ *O*(2×5)+*O*(*n*)。

5 实验与分析

本节利用EXID识别算法对基于IPTAS系统[1]提供的实测数据进行P2P流媒体细粒度识别，而基准数据集是采用L7filter进行标识。

5.1 验证方法

从IPTAS中选定用于验证的IP TRACE，采用L7-filter直接对Trace中5种报文进行打标签，构成标准数据集*A*，将Trace中的UDP报文选出并将其根据流超时参数*T*组成符合FLOWS1格式的流记录集合*Flow*，按第3节中提出的算法完成该*Flow*中各P2P流媒体类型的标记，根据对*Flow*的标记结果完成原始Trace中5种报文的标识，并将所有已标识的报文构建集合*B*，并以此获得该算法的查全率、查准率以及整体正确率。

5.2 评估标准

本文采用常规的流量识别算法的有效评估标准，所涉及的概念有以下几个。

真正TP(true positive)：实际类型为*i*的样本中被分类模型正确预测的样本数。

假正FP(false positive)：实际类型为非*i*的样本中被分类模型误判为类型*i*的样本数量。

假负FN(false negative)：实际类型为*i*的样本中被分类模型误判为其他类型的样本数。

查准率（precision）为

$$precision = \frac{TP}{TP + FP} \tag{1}$$

查全率（recall）为

$$Recall=\frac{TP}{TP+FN} \tag{2}$$

整体准确率（overall accuracy）为

$$overall\ accuracy=\frac{\sum_{i=1}^{n}TP_i}{\sum_{i=1}^{n}(TP_i+FP_i)} \tag{3}$$

5.3　分析数据和验证结果

分析数据为实测的 IP Trace[1]，采集地点是 CERNET 江苏省网边界 10Gbit/s 主干信道。采集时采用了 1/4 的流抽样，但这样的抽样方法对本文的分析结果没有影响。笔者选择了 2 组数据进行分析，第 1 组（ALL_Trace_1）谷时数据采集于 2010 年 5 月 18 号 00:00 ~ 1:00，第 2 组（ALL_Trace_2）峰时数据是当天 19:00 ~ 20:00 的数据。具体参数如表 2 所示，流超时参数 T=16，*ALL_Trace* 的 Flows count 包括 TCP 流。

表 2　　*Trace* 数据描述

Trace	报文数	流数
ALL_Trace_1(0:00-1:00)	3.70×10^8	3.74×10^6
ALL_Trace_2(19:00-20:00)	9.78×10^8	1.12×10^7

表 3　　5 种 P2P 流媒体所占比重

ALL_Trace_1	占总报文数/%	占总字节数/%	占 UDP 报文数/%	占 UDP 字节数/%
PPS 点播	5.12	4.00	12.40	12.78
PPLIVE 点播	2.49	2.04	6.03	6.51
QQLIVE 点播	0.24	0.15	0.59	0.49
UUSEE 点播	0.13	0.14	0.32	0.44
PIPI 点播	0.021	0.025	0.052	0.078
合计	8.00	6.36	19.39	20.30
ALL_Trace_2	占总报文数(%)	占总字节数(%)	占 UDP 报文数(%)	占 UDP 字节数(%)
PPS 点播	6.22	4.89	13.48	12.50
PPLIVE 点播	2.45	1.79	5.31	4.57
QQLIVE 点播	0.44	0.36	0.95	0.91
UUSEE 点播	0.47	0.55	1.02	1.41
PIPI 点播	0.088	0.11	0.19	0.28
合计	9.67	7.70	20.95	19.67

从表 3 可以看出，5 种 P2P 流媒体分别占总 UDP 报文的比重和占总报文的比重，PPS 所占的比重最大，且这 5 种 P2P 流媒体已占总 UDP 报文数或字节数的 20%左右。

根据 5.1 节所提出的验证方法和上述实验数据，获得如下计算结果，具体如表 4 所示。分析过程使用的时间粒度 t 是 5min。

表 4　　5 种 P2P 流媒体的查准率和查全率

评价指标	PPS 点播	PPLIVE	UUSEE	QQLIVE	皮皮点播
查准率	99.5%	98.6%	99.3%	99.4%	99.2%
查全率	97.5%	97.8%	98.7%	98.5%	98.7%
总体正确率	98.5%	98%	98.9%	98.6%	98.2%

从表 4 的结果来看，5 种 P2P 流媒体的识别正确率均达到 97%以上，所采用的实验数据是谷时 ALL_Trace_1 和峰时 ALL_Trace_1 数据的总和。而为了分析 Trace 数据采集在不同时段对分类结果的影响，将其与典型的机器学习算法 C4.5 及 Naivebayes 进行了对比分析。机器学习所采用的测度属性如表 5 所示。在表 5 中列出了 16 种所采用的测度属性，并以此构建机器学习的分类器，在进行机器学习训练前要对这些标记的 TRACE 数据进行组流，并计算上述 16 种测度属性。为了便于对“谷时”和“峰时”2 组数据进行研究讨论，仅选择 5 种 P2P 流媒体数据中的一种——PPS 点播。

表 5　　测度属性及测度说明

流测度	测度说明
双向报文数	两方向报文数之和
双向字节数	两方向字节数之和
平均报文长度	双向字节数 / 双向报文数
持续时间	流结束时间—流开始时间
TOS	两方向 TOS 之 OR
TCPFlags1	某方向流的 TCPFlags
TCPFlags2	另一方向流的 TCPFlags
传输层协议	…
低位端口	…
高位端口	…
PPS	报文数/持续时间
byte/s	字节数/持续时间
平均报文到达间隔	持续时间/报文数
双向报文数比	流中两方向报文数的比率（≥1），其等于双向 PPS 之比和双向报文到达间隔之比
双向字节数比	流中两方向字节数的比率（≥1），其等于双向 byte/s 之比
双向报文长度比	流中两方向报文长度比率（≥1），(字节数 1/报文数 1) / (字节数 2/报文数 2)

从图 2 和图 3 可以看出本方法的查准率指标优于查全率，对“峰时”的效果优于“谷时”。而采用 NAIVEBAYES 和 C4.5 机器学习算法则查准率劣于查全率，并且无论是查准率和查全率都要低于 EXID 识别算法。因为“峰时”的 TRACE 中包含大

量的P2P交互的报文，这样随着样本数的增加，对于识别精度也有所增大。而从下面的分析来看，这个影响的效果比机器学习方法的效果要小。主要是通过分析5种P2P流媒体总体正确率来说明算法的有效性以及样本数对算法的影响。具体如图4所示。

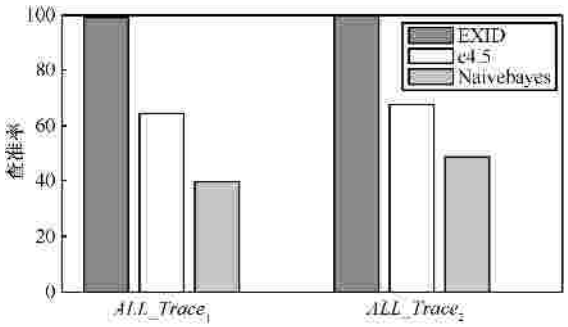

图2 查准率比较

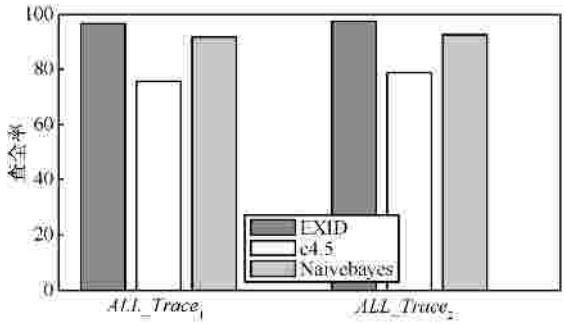

图3 查全率比较

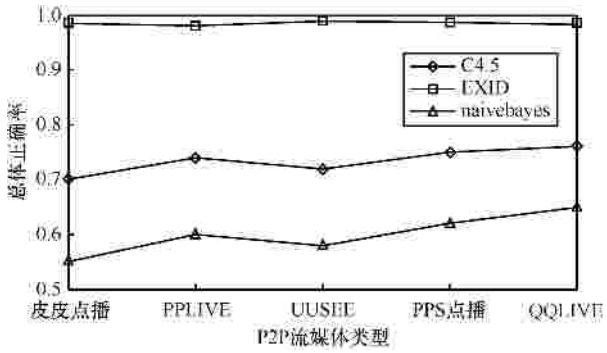

图4 5种常见P2P流媒体的识别整体正确率

从图4可以看到，EXID算法在对5种常见的P2P流媒体的识别总体正确率比其他2个经典的基于机器学习算法要高。更进一步分析发现采用C4.5和NaiveBayes对5种P2P流媒体识别正确率QQLive最高，而皮皮点播的最低。从理论可以分析，由于机器学习对于样本数据的比重较为敏感，而本TRACE数据中数据类型的比重大小排序为QQLive>pps 点播>pplive>UUSEE>皮皮点播，QQLive所占类型比例最大。从图3观察可以得出，采用机器学习的2种识别算法更易受样本比重的影响，同时这也验证了机器学习算法对样本容量大的数据具有较好的识别结果。

涉及到在线流量识别问题，就要考虑到算法的时间效率，因此下面通过对比其他2个经典的机器学习算法来分析EXID算法的时间效率，实验数据采用由1G的TRACE组流得到76 530条流，并通过DPI技术构建NOC_SET标准数据集，具体实验结果如表6所示。

表6 算法时间效率

算法	时间效率/s
NaiveBayes	0.08
C4.5	0.97
EXID	0.001

通过4.3节提到的时间复杂度的分析，并根据实验结果可以得出EXID算法仅使用0.001s时间就完成了5种P2P流媒体的识别。而传统的机器学习方法NaiveBayes和C4.5由于需要对数据集先进行训练然后再进行分类识别处理，这样就耗费了一定的时间，从而对分类的时效性造成了影响。这也是目前机器学习在高速在线的流量识别中所要解决的问题。EXID算法仅采用聚类方法且时间复杂度较低、不需要进行训练。因此具有较高的时间效率。在目前高速在线的流量识别过程中可以考虑采用此解决方案对P2P流媒体流量进行分类识别。

6 结束语

本文通过对流行的P2P流媒体行为特征的分析，提出了一种面向P2P流媒体应用的UDP流量识别方法，经对包含5种典型的P2P流媒体电视数据进行识别，其实验结果表明所提出的EXID算法具有很高的查全率和查准率，而且时间复杂度低，在其使用的扩展流记录格式能够满足的条件下，可实现在线识别。并且通过和经典的机器学习算法的比较，结果表明：

1) 具有更高的识别精度和整体的识别率；

2) 不易受样本比重的影响，这样就可以把抽样的影响降到最低。

本文的研究工作也对其他路由器或具备流记录生成能力的制造厂商在定义自己流记录格式时具有参考意义。

本文提出的基于最大最小报文长度的识别方

法是从满足在线识别角度出发设计的，而这些最大最小报文并不是实际中使用频数最高的。如果不考虑时间复杂度的代价，仅从提高识别准确率的需求考虑，按本文的思路，通过设计更复杂的测度标准可以设计出更好的算法，这些算法可以用于静态 IP Trace 的分析，是今后工作的一个目标。

参考文献：

[1] IP trace distribution system[EB/OL].http://iptas.edu.cn, 2010.

[2] 张艺濒,张志斌,赵咏等.TCP 与 UDP 网络流量对比分析研究[J].计算机应用研究,2010,27(6):2192-2197.
ZHANG Y B, ZHANG Z B, ZHAO Y, *et al*. TCP and UDP network traffic comparison analysis[J]. Application Research of Computers, 2010, 27(6):2192-2197.

[3] LEE D, CARPENTER B E, BROWNLEE N. Observations of UDP to TCP ratio and port numbers[A]. Proc Int Conf on Internet Monitoring and Protection (ICIMP)[C]. Barcelona, Spain, 2010.99-104.

[4] Tcpudpratio[EB/OL].http://www.caida.org/research/traffic-analysis/tcpudpratio, 2009.

[5] 樊华,李理,袁坚等.互联网流量控制的朗之万模型及相变分析[J].物理学报,2009,58 (11) :7507-7513.
FAN H, LI L, YUAN J, *et al*. Langevin model of the flow control in the internet and its phase transition analysis[J]. Acta Physica Sinica, 2009, 58 (11):7507-7513.

[6] Coralreef[EB/OL].http://www.caida.org/tools/measurement/coralreef, 1999.

[7] ROUGHAN M, SEN S, SPATSCHECK O, *et al*. Class-of-service mapping for QOS: a statistical signature-based approach to IP traffic classification[A]. Proc of the ACM SIGCOMM Internet Measurement Conf[C]. Taormina, Italy, 2004. 135-148.

[8] MOORE A W, ZUEV D. Internet traffic classification using Bayesian analysis techniques[A]. Proc of the 2005 ACM SIGMETRICS Int'l Conf on Measurement and Modeling of Computer Systems[C]. Banff, Alberta, Canada, 2005. 50-60.

[9] 李君, 张顺颐, 王浩云等. 基于贝叶斯网络的 Peer to peer 识别方法[J]. 应用科学学报, 2009, 27 (2):124-130.
LI J, ZHANG S Y, WANG H Y, *et al*. Peer to peer identification using Bayesian networks[J]. Journal of Applied Sciences, 2009, 27(2): 124-130.

[10] 徐鹏, 刘琼, 林森. 基于支持向量机的 Internet 流量分类研究[J].计算机研究与发展, 2009, 46 (3):407-414.
XU P, LIU Q, LIN S. Internet traffic classification based on support vector machines[J]. Journal of Computer Research and Development, 2009, 46 (3):407-414.

[11] KARAGIANNIS T, PAPAGIANNAKI K, FALOUTSOS M. BLINC: Multilevel traffic classification in the dark[A]. Proc of the ACM Sigcomm[C]. Philadelphia, USA, 2005. 229-240.

[12] L7-filter, application layer packet classifier for Linux[EB/OL]. http://l7-filter.sourceforge.net, 2003.

[13] 胡超,陈鸣,许博等. 一种基于爬虫的分布式 PPLive 流实时检测系统[J]. 解放军理工大学学报,2008,9(5):512-516.
HU C, CHEN M, XU B, *et al*. Reptiles distributed PPLive streaming real-time detection system[J]. Journal of PLA University of Science and Technology (Natural Science Edition). 2008, 9(5):512-516.

[14] Cisco system, IOS netflow feature(S)[EB/OL]. http://www.cisco.com/warp/public/732/Tech/nmp/NetFlow/, 2004.

[15] 胡超. 一种 P2P 流识别和分析系统的设计与实现[D]. 南京:解放军理工大学, 2008.
HU C. Design and Implementation of a P2P Flow Identification and Analysis System[D]. Nanjing: PLA University, 2008.

[16] BLEUL H, RATHGEB E P, ZILLING S. Advanced P2P multiprotocol traffic analysis based on application level signature ion[A]. Proc of the Telecommunications Network Strategy and Planning[C]. New Delhi, India, 2006.1-6.

[17] XU K, ZHANG M, YE M J, *et al*. Identify P2P traffic by inspecting data transfer behavior[J]. Journal of Computer Communi ions, 2010, 33(10):1141-1150.

[18] LIU X B, YANG J H, XIE G G, *et al*. Automated mining of packet signatures for traffic identification at application a with apriori algorithm[J]. Journal on Communications, 2009, 30(12):51-59.

[19] TEUFL P, PAYER U, AMLING M, *et al*. InfeCT-network traffic classification[A]. Proc of the 7th Int'l Conf on Networkin (ICN)[C]. Cancun, Mexico, 2008. 439-444.

[20] PERÉNYI M, MOLNÁR S. Enhanced skype traffic identification[A]. Proc of the 2nd Int'l Conf on Performance Evaluation Methodologies and Tools[C]. Brussels, Belgium, 2007. 1-9.

[21] BONFIGLIO D, MELLIA M, MEO M, *et al*. Revealing skype traffic: when randomness plays with you[A]. ACM SIGCOMM Computer Communication Review[C]. New York, USA, 2007. 37-48.

[22] YANG A M, JIANG S Y, DENG H. A P2P network traffic classification method using SVM[A]. Proc of the 9th Int'l Conf for Young Computer Scientists (ICYCS 2008)[C]. Zhangjiajie, China, 2008. 398-403.

[23] ESTE A, GRINGOLI F, SALGARELLI L. On the stability of the information carried by traffic flow features at the packet level[A]. ACM SIGCOMM Computer Communication Review[C]. New York, USA, 2009. 13-18.

[24] ESTE A, GRINGOLI F, SALGARELLI L. Support vector machines for TCP traffic classification[J]. Computer Networks, 2009, 53(14): 2476-2490.

[25] ROUGHAN M, SEN S, SPATSCHECK O, *et al*. Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification[A]. Proc of the 4th ACM SIGCOMM Conf on Internet Measurement[C]. New York, USA, 2004. 135-148.

[26] MORI T, UCHIDA M, GOTO S. Flow analysis of Internet traffic: world wide web versus peer-to-peer[J]. Journal Systems and Comput-

ers in Japan, 2005,36(11):70-81.

[27] BASHER N, MAHANTI A, WILLIAMSON C, *et al.* A comparative analysis of Web and peer-to-peer traffic[A]. Proc of the 17th Int'l Conf on world wide web[C]. New York, USA, 2008. 287-296.

[28] CHEN Q Z, SHAO B, CHEN C. Design and implementation of P2P traffic identification system based on compound characteristics[J]. Journal of Southeast University (Natural Science Edition), 2008, 38(S1): 109-113.

[29] MOORE A W, ZUEV D. Internet traffic classification using bayesian analysis techniques[A]. ACM SIGMETRICS Performance Eva uation Review[C]. New York, USA, 2005. 50-60.

[30] LI W, CANINI M, MOORE A W, *et al.* Efficient application identification and the temporal and spatial stability of classification schema[J]. Computer Networks, 2009, 53(6):790-809.

[31] ERMAN J, MAHANTI A, ARLITT M, *et al.* Offline/realtime traffic classification using semi-supervised learning[J]. Performance Evaluation, 2007, 64(9-12):1194-1213.

[32] SEN S, SPATSCHECK O, AND D. WANG accurate, scalable in-network identification of P2P traffic using application signatures[A]. in WWW[C]. New York, USA, 2004. 512-521

[33] KARAGIANNIS T, BROIDO A, FALOUTSOS M. Transport layer identification of P2P traffic[A]. Proc of International Measurement Conference[C]. Sicily, Italy, 2004.121-134.

[34] **鲁文斌,杨家海,刘洪波.基于节点连接模式的** P2P **节点识别算法**[J]. **清华大学学报(自然科学版)**,2009, 49(7):1045-1049.
LU W B, YANG J H, LIU H B. Identification of P2P peers based on connection patterns[J]. Journal of Tsinghua University (Natural Science Edition), 2009, 49(7):1045-1049.

作者简介：

董仕（1980-），**男，河南周口人，东南大学博士生，主要研究方向为网络测量与网络行为学。**

王岗（1986-），**男，山东潍纺人，东南大学硕士生，主要研究方向为网络管理。**